A NOVEL SCHEME FOR SECURE KEY GENERATION THROUGH FINGER VEIN PATTERN

Research Proposal submitted

In partial fulfillment of registration to

Ph.D. Program

In the subject of Computer Science
Faculty of Science & Technology

Submitted by

Mrs. Dnyaneshwari P. Wagh

Under the Guidance of

Dr. G. N. Shinde
Pro - Vice Chancellor
S. R. T. M. U. Nanded

Co-Guide
Dr. H.S. Fadewar
School of Comp.Sci
S. R. T. M. U. Nanded
Nanded– 431606 (Maharashtra) India

Swami Ramanand Teerth Marathwada University, Nanded
February 2018

Table of Contents

Sr. No.	Contents	Page No.
	Abstract	1
1	Introduction	2
2	Review of Literature &Development in the Subject	3
3	Statement of the problem	6
4	Research Objectives	7
5	Research Methodology	7
6	Significance of study	9
7	Proposed work design / Formulation and structure of study	11
8	References	12

A NOVEL SCHEME FOR SECURE KEY GENERATION THROUGH FINGER VEIN PATTERN

Abstract:

Information security is becoming more and more important. The PINs and passwords work as cryptographic keys that are easy to forget or vulnerable or forgery. Cryptography is one of the most effective ways to solve the problem of information security. In the cryptographic algorithms information is encrypted and decrypted using cipher key. Simple key user is easy to remember but they can also easy to crack. Complex keys are deficit to crack but they are difficult to remember as well and may have to be stored in medium that could get lost or stolen. The biometric features which cannot be forgotten, stolen or cracked. One of the newest biometric feature is finger vein. The finger vein pattern based authentication method is highly reliable and secure. Finger vein are hidden under the skin surface, so forgery is extremely difficult. Unique aspects of finger vein pattern recognition set this method apart from other forms of biometrics. The finger vein technology is More suitable for used by the older population compared to fingerprint.

Bio-cryptography is a progressive technology that combines biometrics with cryptography. Biometric system use for security purpose has become increasingly popular. The use of biometric data in cryptography is a new growing and promising area of research. The encryption key generation is the big problem in biometric.

Finger vein are a promising biometric pattern for personalized identification in terms of their advantages over existing biometrics. The method of key generation from finger vein pattern it is based on the established finger vein image pre-processing methods and a new algorithm. Experiments are performed on a Finger vein database to verify the feasibility of the proposed method.

Keywords: Biometrics, cryptography, Information Security, Encryption, Decryption, Cryptographic Key Generation, Authentication.

1. Introduction:

Now a day the life is very fast. We want to do everything so quickly and easily without taking many physical and metal efforts. Information security and a secure transmission of data become very important. So, to keep our information secretly we use secret password but such passwords can be forget, cracked by hackers. To avoid such problems we must use biometric unique identities. Biometric systems recognize a person based on his physical or behavioral characteristics i.e. fingerprint, face, iris, signature, finger vein, voice etc. By the invention of these characteristics are strongly bond to the person, biometrics provide high degree of assurance about his identity. A number of biometric characteristics are being used in various applications such as Uniqueness, Permanence, Measurability, Performance, Universality, Acceptability and Circumvention [2]. The most common physical biometric patterns used for security purpose. With the diffuse use of information exchange across the internet and storing the sensitive data on open networks, cryptography plays a major role for providing security.

Cryptography acts in an effective way to solve the problem of data security. Cryptographic key is capable of providing better user authentication and better security. Most of the cryptographic algorithm, cipher keys are used for encryption and decryption. But this causes some problems[3]. Simple user keys are not easy to be forget. But, they can be cracked easily. But on moving to the case of complex keys, even though they are difficult to check, they are difficult to remember. Also, the cipher key may be illegally shared. So, these entire problems should be solved. The biometric features which cannot be forgotten, stolen or cracked, is combined with the cryptography to form biometric cryptography [1].

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity.

2. Review literature:

In 2004, Yoo- Jen Chang, Wende Zhang and Tsuhan Chen, in paper title "Biometric based cryptographic key generation ", In this paper Proposed framework differs from prior work in that user-dependent transforms are utilized to generate more compact and distinguishable features. Thereby, a longer and more stable bit stream can be generated as the cryptographic key. Experiments are performed on a face database to verify the feasibility of the proposed framework.

In 2005, Naoto Miura et al, in paper " Extraction of Finger vein patterns Using Maximum Curvature Points in Image Profiles", proposed a biometric system for identifying individuals using vein pattern. The verious widths and brightnesses that change temporally as a result of fluctuation in the amout of blood in vein, temprature, physical conditions etc. He develop a method of calculating local maximum curvature in cross sectional profiles of vein.

In 2007, B. Chen, in paper " Biometric based Cryptographic key generation from face", In this Paper discusses a new method which sees an entropy based feature extraction process coupled with reed – Solomon error correcting codes that can generate deterministic bit-sequences from the output of an integrative one-way transform. The technique is evaluated using 3D face data and is shown to reliably produce keys of suitable length for 128-bit Advanced Encryption Standard (AES).

In 2007, Christopher et al in paper "Active Biometric Cryptography :Key generation Using Feature and Parametric Aggregation", introduced key generation mechanism are responsible for some of the more common security weaknesses affecting many information system. He has done demonstrating the use of biometrics to produce cipher keys. The other approaches require complex data processing to recover the cipher key. These approaches demonstrates how a cryptographic key can be constructed through the use of biometric features and parametric aggegation along with certain mathematical combinatorial and Permutation constructs.

In 2008, David et al, in paper " A study of Finger vein biometric for Personal Identification", proposed the process to enhance the image qality that worsen by light effect and produces noise by the camera, then segment the vein pattern by using threshold method and matched them using improved templet matching. The result shows good quality.

In 2010, A. Jagadeesan, T. Thillaikkarasi and K. Duraiswamy, in paper "Cryptographic key generation from mltiple biometric modalities: fusing minutiae with Iris Feature", In this paper introduce way to use biometric features of the user rather than memorable password in an attempt to produce through and repeatable cryptographic key. Generated 256 bit cryptographic key is capable of providing better user authentication and better security.

In 2010, A. Jagadeesan and K. Duraiswamy, in paper "Secured cryptographic key generation from multimodal biometrics: Feature level fusion of Fingerprint and Iris", In this paper he say that an approach to incorporate the volatility of users biometric feature into generated key. Multiple biometrics modalities into cryptographic key generation so as to provide better security. For experimentation they use iris images from CASIA Iris database and fingerprint images from publically available. The result gives better effectiveness.

In 2012,Shaifah Muntazah syed Ahmad and Wan Azizun wan Adnan, in paper "Technical issues and challenges of biometric applications as access control tools of information security", In this paper he focused on technical issues and challenges faced by biometric technologies within the application of information security.

In 2012, P. Balakumar and R. Venkatesan, in paper " A survey on Biometrics based cryptographic key generation schemes", In this paper he introduce the several biometrics like fingerprint, iris, retina, etc are used in rendering security to the information key. This servey discussed the several biometrics based cryptographic key generation schemes which will show the way for development of better security schemes using biometrics and cryptography.

In 2012, Zhi Liu et al, in this paper "An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices", introduced areal time embeded finger vein

recognation system athentication on mobile devices. The system is implemented on DSP platform and equipped with a novel finger vein recognation algorithm.

In 2015, Anil K. Jain, Arun Ross and Umut Uludag, in paper "Biometric template security: challenges and Solution", In this paper he say that various threats that can be encountered by a biometric system. They specifically focus on attacks designed to elicit information about the original biometric data of an individual from the stored template. They provide experimental results pertaining to a hybrid system.

In 2015, Saad Abuguba, Milan M. Milosavljevic and Nemanja Macek, in paper "An Efficient approach to Generating Cryptographic Keys from face and Iris Biometrics at the Feature level", In this paper Introduce biometric cryptographic system designed to generate a cryptographic key from a biometric trait, incorporate high level of security provided by cryptography and non repudiation provided by biometry as well as elimination the need for a user to remember long passwords or carry tokens.

In 2015, J. Chavez- Galaviz et al in paper, "Embedded biometric cryptosystem based on finger vein patterns", proposed algorithum for the location of vein intersection point and the quantification of the angles between the vein-branches. Using this information they generate a personal key that allow the user to encrypt information after the authentication is approved.

In 2016, Sharon Davis, Ayana John and Padmam Kaimal, in paper " Cryptographic key generation from finger vein; A study", In this paper he say that biometrics in conjunction with cryptography forms a new progressive technology using finger vein. It is based on the established finger vein image pre-processing methods and new algorithm.

In 2016, Sanjay Kanade, Dijana Patrovska - Delacretaz, and Berandette Dorizzi, in paper "Multi-Biometrics based cryptographic key regeneration scheme", In this paper he Propose a multi-biometric based cryptographic key regeneration scheme. Since left and right irises of a person are uncorrelated, we treat them as two independent biometrics and combine in

our system. We propose a novel idea for feature level fusion through weighted error correction to obtaine a multi-biometric feature vector which is used to get a secure template.

In 2016, Fatame Saadat et al in paper, "A GSA- based method in Human Identification Using Finger vein Patterns", proposed a heuristic method for score level fusion of three different finger vein's pattern. The multibiometric system, Gravitational Search algorithum is used to tune the weights of sum fusion strategy.

In 2017, A. Ruba, G Rajkmar and K. Parinala, in paper " Biometrics based Cryptographic key generation using finger print", In this paper they implement cryptographic key senders recent fingerprint would be used to construct key by combining it with information for key decryption the senders database fingerprint images which are previously kept by receivers end would be used.

In 2017, Liukui Chen et al " A Finger vein Image-Based Personal Identification Systems With Self- Adaptive Illuminance Control", introduced an observation model of finger vein imaging, upon which a self adaptive illminance control algorithum.the algorithum could automatically adjust the illuminance distribtion of light. With this adaptation, the whole finger body could be illuminated appropriately according to its thickness distributionand the overexposure and underexposure are avided properly.

3. Statement of the problem:

Now a day it is major problem to secure our most important information. While the transfer of information from one person to another sometimes subject information can be trap by someone. There were many keys invented to secure the information but total security system yet not developed. This problem is focused in our mind, our research is proposed to strong key generation for security template.

4. Research Objectives:

- To study and identify the best biometric techniques for information security when data is transfer from source to destination.
- To study Finger vein biometric pattern for personalized identification in terms of their advantages over existing biometrics
- To develop hypothesis supporting a security template for user Authentication using finger vein pattern recognition.
- To generate strong biometric key using finger vein, it could not be break easily from unauthorized users.
- Implementing & testing Finger Vein security system on different test modules.

5. Research Methodology:

1) The proposed research focused on Biometric security system. Biometric cryptosystems combines cryptography and biometrics to afford the advantages of both for secrity. This technique will provide the advantages like better and modifiable security levels which are the advantages of cryptography and advantages like eliminating the must to memorize passwords or to carry yokes etc. Which are the advantages of using biometrics?

The important step in finger vein recognition is the vein extraction from the background. The finger vein images are acquired by the use of NIR spectroscopy. The NIR spectroscopy appears to be darker than other region of the finger. This is because the blood vessels alone will absorb the rays.

The performance of the finger vein extraction and matching algorithm depend upon the quality of image. The image is enhanced to eliminate the noise using oriented filter method. This also enhances the ridgelines and uses Gabor filter.

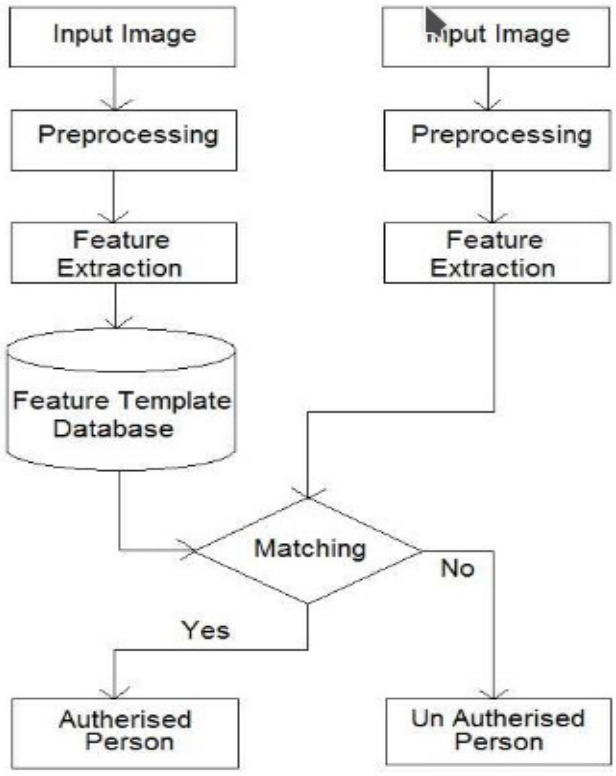

Fig 1: Finger Vein security system

2) In this method cryptographic key generation from finger vein pattern demonstrated. A schematic representation method form finger vein patterns. Using finger vein pattern, key is generated. Biometric method is combined with a password. The password is 'entered' by provide different finger sequences for the systems. Then different finger vein patterns and combinations of enrolling these images to the system allows for virtually endless number of keys to be generated. Also longer keys and keys with higher entropy can be generated. First, vein pattern image is processed using conventional methods. Input to Contour Tracing Algorithm is the processed vein pattern and it is used to generate a partial cryptographic key. Partial cryptographic keys are concatenated to combine a final cryptographic key. Finger vein pattern

may be cropped depending on its sizes that we are able to make sure that to vein beginning and end points reach edges of the image.

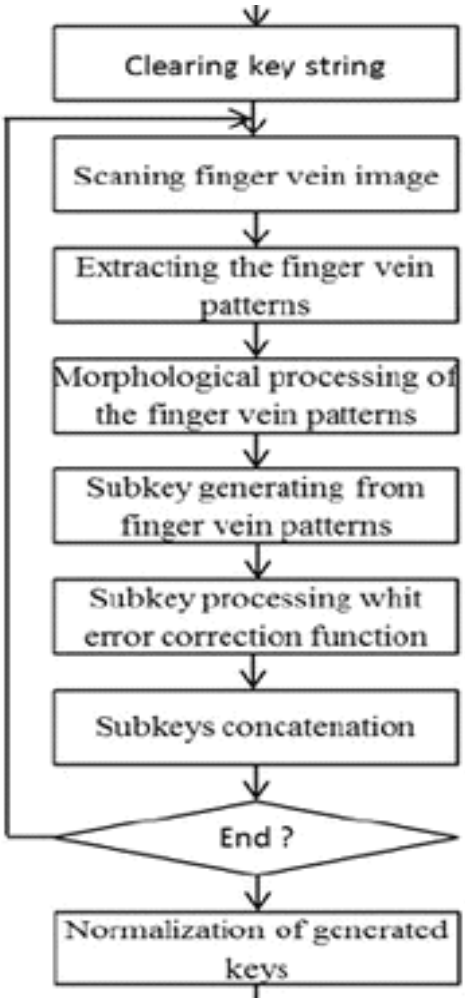
Clearing key string
Scaning finger vein image
Extracting the finger vein patterns
Morphological processing of the finger vein patterns
Subkey generating from finger vein patterns
Subkey processing whit error correction function
Subkeys concatenation
End ?
Normalization of generated keys

Fig. 2: Schematic representations of proposed cryptographic key generation method using finger vein pattern.

6. Significance of the study:

A Biometric device is a security identification and authentication device. Such devices use automated methods of verifying or recognizing the identity of a living person based on a

physiological or behavioral characteristic. These characteristics include fingerprints, facial images, Iris prints, Finger vein and voice recognition.

1) Use to secure national information.
2) Hackers cant hake secret information easily.
3) Finger is the Unique identity.
4) Without permission of user Know one can get the information.

6.1. International status:

Focuses on selected international Status areas like UID, Bank, ATM machine, Airport, Railway, Smart phone, Information security, Door locks, Military etc.

6.2. National Status:

Focuses on selected international Status areas like UID (Adhar), Government schemes, Bank, ATM machine, Airport, Railway, Smart phone, Information security, Door locks, Military etc.

7. Proposed work design / formulation and structure of study:

The Work plan is written in the phases such as

Phase 1: In first six month we will collect the data and study of various methodologies that used for secure biometric system generation

Phase 2: In next six month we will done practical implementation.

Phase 3: In next four month we will done analysis of data and conclusion

Phase 4: In next six month we write the report.

Phase 5: In Last two month, correction and other work.

8. References:

[1] Sharon Davis, Ayana John, Padmam Kaimal, " Cryptographic key generation from finger vein; A study", IOSR Journal of electronics and communication engineering, e-ISSN: 2278-2834.

[2] Junichi Hashimoto, " Finger vein Authentication Technology and its Future", IEEE, 2006.

[3] Zhi Liu and Shangling Song, "An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices", IEEE Transaction on Consumer Electronocs, Vol.58, No.2, May 2012.

[4] Christopher R. Costanzo, "Active Biometric Cryptography :Key generation Using Feature and Parametric Aggregation", IEEE, 2007.

[5] A. Jagadeesan, K. Duraiswamy and T. Thillaikkarasi, " Cryptographic key generation from mltiple biometric modalities: fusing minutiae with Ieis Feature", International Journal of Computer applications (0975-8887) Vol.2 – No.6, June 2010.

[6] Naoto Miura, Akio Nagasaka, " Extraction of Finger vein patterns Using Maximum Curvature Points in Image Profiles", IAPR Conference on Machine Vision applications, May 2005.

[7] Naoto Miura, Akio Nagasaka, " Automatic Feature Extraction from non-uniform Finger vein Image and its Applications to Personal Identification", IAPR Workshop on Machin Vision Applications, Dec 2011.

[8] Fatame Saadat, Mehdi Nasri, "A GSA- based method in Human Identification Using Finger vein Patterns", IEEE, 2016.

[9] Yoo-Jen Chang, Wende Zhang and Tsuhan Chen, " Biometric based cryptographic key generation", IEEE 2004.

[10] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil Jain, " Biometric Cryptosystems : Issues and Challenges" , IEEE, Vol. 92, No.6, Jne 2004.

[11] Sharifah Muntazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan, " Technical issues and challenges of biometric applications as access control tools of information security", International Journal of Innovative Computing, Information and Control – Vol.8, No.11, November 2012.

[12] P. Balakmar, R. Venkatesan , " A survey on Biometrics based cryptographic key generation schemes", International Journal of computer science and Information Technology ans Security, Vol.2, No.1, 2012.

[13] Liukui Chen, Jing Wang, " A Finger vein Image-Based Personal Identification Systems With Self- Adaptive Illuminance Control", IEEE Transactions on Instrumentation and Measurement, Vol.66, No.2, February 2017.

[14] Saritha Reddy Venna, Ramesh Babu Inampudi, " A Novel method for Cryptographic key generation Fusion Dual Finger Vein Images", International journal of Computer science and information Technologies, Vol.7, 2016.

[15] David Mulyono, Horng Shi Jinn, " A study of Finger vein biometric for Personal Identification", IEEE International Symposium on Biometrics and Security Technologies, 2008.

[16] A. Venckauskas, N.Morkevicis, K. Kulilauskas, "Study of Finger vein authenticationalgorithms for physical access control", Electronic and Electrical Engineering, No.5, 2012.

[17] Shruthi B.M, Pooja Mohnani, Ashwin R.G, "Multimodal Biometric Authentication Combining Finger Vein and Finger Print", International Journal of Engineering Research and Development, Vol.7, Issue10, July2013.

[18] J.Chavez-Galaviz, J.Ruiz-Rojas, A. Garcia-Gonzalez, "Embedded biometric cryptosystem based on finger vein patterns", IEEE Xplore, 2015.

[19] Wenming Yang, Qing Rao, and Qingmin Liao, " Personal Identification for Single Sample using finger vein location and Direction Coding", Proceeding of the IEEE international Conference on Hand-based Biometrics, March 2011.

Signature	Signature	Signature
Mrs. Dnyaneshwari P.Wagh	**Dr. H.S. Fadewar**	**Dr. Shinde G. N**
Research Scholar	Research Co-Guide	Research Guide